Planned U.S. sensor network targets terror threats

By Rick Merritt, EE Times
July 14, 2003 (11:52 a.m. EST)
URL: http://www.eetimes.com/story/OEG20030714S0049

SAN MATEO, Calif. — Against the backdrop of the war on terrorism, an expanding group of government researchers is at work on a nationwide sensor network that someday could provide a real-time early-warning system for a wide array of chemical, biological and nuclear threats across the United States.

Drafts of the objectives and milestones for the sensor network project are already circulating among key scientists at national labs and within an emerging technology branch inside the newly formed Department of Homeland Security that is coordinating the effort. While details of the program are not likely to be made public until at least this fall, the national labs have been working for more than a year on the core issues in materials, sensors, networks and electronics, and already have set up several field trials of prototype networks.

Project researchers hope to use microelectromechanical systems (MEMS) and nanotechnology to create a suite of low-cost yet highly accurate biological and chemical sensors. On the networking front, they foresee an Internet-like peer-to-peer network with multilevel security and quality-of-service guarantees, spanning wireless, wired and satellite links.

Backers are divided on the impact the project might have on commercial markets (see story, below). Some believe the opportunities will be huge, while others say it's simply too early to tell.

In the aftermath of 9/11 and the anthrax attacks that followed, researchers at the national labs saw a multifaceted threat unfolding. Potential targets include airports, subways and buildings as well as water sources, animal herds and flocks of birds that could spread contaminants or harmful biological agents.

"A lot of us thought, holy mackerel, how will we handle this?" said C. Robert Kline Jr., general manager of Hytec Sensors & Imaging Group Inc. The Los Alamos, N.M., company handles systems integration for sensor networks and is working on two classified projects.

The list of possible biological and chemical agents to detect is maddeningly diverse. One agency has published a roster of about 50 biological agents alone (see www.niaid.nih.gov/biodefense/bandc_priority.htm). The multifaceted nature of the threat led researchers to conclude the network will consist of a suite of different kinds of sensors.

"Some people want to find one little box that will do everything, but we need to focus on a family of technologies," said Gary Resnick, program manager for chemical and biological threat reduction at Los Alamos National Labs. He estimates that 40 percent of an over-all government allocation of $2 billion to $3 billion will fund new detection systems.

"The thing we are trying to detect is evolving over time. It's a dynamic, abnormal needle in

a haystack, and it's hard to develop a device that doesn't give false positives or negatives," Resnick said.

In one approach, researchers are studying hybrid sensors that use surface-chemical detection as a first step, or trigger, that could be followed up with more expensive and time-consuming techniques such as DNA testing on the same device. Others are studying the use of infrared or ultraviolet spectrum analysis as well as biometric sensors that mimic human cells to create test reactions.

Further into the future, MEMS technology is seen as having promise for creating miniature benchtop labs on a chip. At the same time, other teams are exploring nanotechnology to deliver new sensor materials.

"It's too soon to down-select, but I am personally very excited about the potential for nanotechnology to provide a detection capability that is very cost-effective," said Resnick. "We are looking for breakthroughs in this area."

More than 50 researchers at Pacific Northwest National Laboratory (Richland, Wash.) have been developing nanosize preconcentrators for nerve agents, botulism and other toxins. The group starts work in October on the electronics portions of its sensors, said Doug Lemon, leader of the Homeland Security initiative at the lab.

The goal for all the government efforts, perhaps three to five years out, is to deploy a highly accurate yet low-cost network of sensors "that in a couple of minutes could tell you if an agent is present, in what concentration and something about the agent. But the technology for that doesn't really exist yet," said Duane Lindner, director of chem/bio programs at Sandia National Labs (Livermore, Calif.), where more than 100 developers have been at work on sensor networks.

Sandia hopes to prototype by fall 2004 a sensor that could detect chemicals such as nerve and blister agents as well as some top-priority industrial toxins. The sensor would use polymer- or gel-coated silicon devices to trap targeted chemicals, then send the agents through fluidic channels to on-chip arrays of surface-acoustic-wave detectors running at up to 500 MHz. A follow-on device would integrate the fluidics, SAWs and support electronics on a single device.

"It's a challenge getting exquisitely sensitive SAWs that can run on battery power," said Lindner.

Sandia is now testing handheld sensors designed to detect within two minutes chemical-weapons agents on the battlefield with what researchers call "unprecedented sensitivity." The lab has been asked to explore adding networking and GPS capability to those sensors so they could be mounted on military vehicles, creating a mobile battlefield sensor network.

Perhaps five to six years from now, "we will have a bio smoke alarm that will be in our homes and airports, but that's a ways off," said Resnick.

At Oak Ridge National Labs in Tennessee, meanwhile, a team of researchers has been working for 18 months on an underlying network architecture for a national sensor network. The group anticipates a "medium-size" Department of Defense grant this summer to expand its SensorNet program, said Brian Worley, director of the computational science and engineering division at Oak Ridge.

The team will develop and test the networking architecture over the next year, then follow up with a metro-area trial. The SensorNet project, running on a $3 million budget this year, is seeking $9 million in funding for its next fiscal year.

Developing quality-of-service guarantees and multilevel security for a hybrid wired, wireless and satellite network will be the primary challenge, said Worley. The group will use off-the-shelf technology as much as possible and hopes to leverage existing infrastructure such as the 30,000 cellular towers and 100,000 cellular basestations in the United States today.

That represents an opportunity for Flash Technology (Franklin, Tenn.), which services aviation warning lights on towers across the nation. Looking to expand into security and environmental businesses, the company became a strategic partner with Oak Ridge after it heard about the lab's work in sensor networks.

The two collaborated in a March 2002 trial of a three-site sensor network. The test successfully detected an agent and within 96 seconds sounded a warning that included estimates of affected population centers from projected plume movements based on weather data.

A host of pilot sensor network projects are in field tests, including systems developed by Los Alamos and Berkeley researchers to safeguard crops. "We do have sensors out in fields originally developed to track the spread of insecticides and fertilizers," said Kline of Hytec.

Trial sensor networks also are in place in Boston subways, at the San Francisco airport and on the Miami docks. The Washington subway recently went operational with a chemical-sensor system developed by Sandia and Argonne National Labs in Chicago. Sandia, which is managing at least two other sensor net test beds, plans a significant demonstration of a wireless network next spring as well as a test of a bio sensor net this fall.

The authority for a national sensor network flows from the Department of Homeland Security (DHS), which has been charted to develop chemical, biological, nuclear, explosive and cyber protection plans. Draft objectives of that plan are already being circulated and could be made public when the new fiscal year begins in October.

DHS is in the process of forming its own science-and-technology directorate under Charles E. McQueary, a former division president of General Dynamics, who was named undersecretary for the DHS unit earlier this year.

President George W. Bush's 2004 budget, released in February, includes about $1 billion in funding for internal research and development at DHS. About 80 percent of that R&D money will be under the control of the DHS science-and-technology unit. DHS is also creating a Homeland Security Advanced Research Projects Agency, modeled after the Pentagon's Darpa, to commission and coordinate external research. That agency will have an estimated $340 million budget in fiscal 2004.

In addition, the directorate is also expected to set up a 20-person advisory council, a Homeland Security Institute that will act as a think tank and a number of university-based research centers, according to an analysis by the American Association for the Advancement of Science.

"It will take months before the new department has the leadership and capabilities to flesh out its science and technology infrastructure," said the AAAS report.

Indeed, these are "exciting and challenging" times for the people pulling together from "scratch the technical underpinnings of DHS," said Lindner of Sandia Labs. "I spent some time in the Washington office, where even tracking down a stapler is a major project. They are building a bridge while trying to drive trucks across it."